CCY4301
Cyber-Physical Systems Security

Fall 2025

Dr Ashraf Samy

Lecture 1
Introduction to Cyber-Physical Systems

1.1 Cyber-Physical Systems (cont.)

This lecture summarizes the forgoing mentioned knowledge to introduce cyber physical systems with regard to the existing manifold of definitions such as:

- **Systems of collaborating computational elements controlling physical entities.**
- **Networks of interacting elements with physical inputs and output instead of a stand-alone device.**
- **Internet of Things, Data, and Services**
- **Interconnections between physical and virtual world models**
- **Ability for autonomous behavior such as self-control and/or self-optimization**
- **Internet-based business models, social networks, and communities**
- **System of systems**
- **New way of cooperation among distributed and intelligent smart networked devices as well as with humans**

1.1 Cyber-Physical Systems (cont.)

From these definitions, it can be stated that cyber-physical systems span a wide range from the miniscale, e.g., pacemakers, to the large scale, e.g., power grids, in their diversity of applications, because the ubiquity of computer devices is a huge source of economic leverage.

- From the history in cyber-physical systems, it should be noted that in 2006, the National Science Foundation (NSF) in the USA has identified cyber-physical systems (CPSs) as one of the promising research themes of the future.
- In the following year, based on the recommendation of the President's Council of Advisors on Science and Technology (PCAST) (PCAST 2007), a research program was established by the NSF titled Cyber-Physical Systems, in which about 65 projects amounting to almost 60 million US$ have been funded.
- In a subsequent report of PCAST in 2010, further research needs for cyber-physical systems were expelled, and the related NSF program initially extended until 2013, with a budget of over 30 million US$.

1.1 Cyber-Physical Systems (cont.)

- In the year 2012, a study funded by the Federal Ministry of Education and Research in Germany (BMBF) was published by the German Academy of Science and Engineering (acatech) on the topic information and communication technologies (ICTs), which was tied to the megatrend Internet of Things which addresses the opportunities and challenges of the technology trends of cyber physical systems (Geisberger and Broy 2012).
- According to these studies, cyber-physical systems will play an essential role in industry and society leading to breakthroughs in all relevant areas by bridging the wide range of fields of action in which cyber-physical systems can be applied. The reason for that is that cyber-physical systems go beyond traditional systems (see Chaps. 1 and 2) employed in industry in their complexity, such as automation systems, which require a much closer networking of the appropriate systems and software engineering disciplines.

1.1 Cyber-Physical Systems (cont.)

- Traditionally automation systems networking is carried out through specially developed network structures like PROFIBUS (Process Field Bus), DP (Decentralised Peripherals), used to operate sensors and actuators via a centralised controller in production automation applications, and PA (Process Automation), used to monitor measuring equipment via a process control system in process automation applications.
- In contrast, cyber-physical systems usually use open network technologies like the Internet. The massive importance of growth of the Internet is characterized by the Internet of Things (IoT) (see Chap. 4; M€oller 2013) in which the real and the virtual worlds are converging.

1.1 Cyber-Physical Systems (cont.)

- Thus, cyber-physical systems, which are based on converging real (physical) and virtual (cyber) systems, gain a growing importance in networking of embedded computing systems (see Chap.2) and components of the information and communication technology (ICT) as well as with the Internet or more in general, the Internet of Things as a dynamic global network infrastructure with self-configuring capabilities based on a standard and interoperable communication protocol, the Internet Protocol version 6 (IPv6).
- The IPv6 is the latest version that routes traffic across the Internet. It was developed by the Internet Engineering Task Force to replace the IPv4 to overcome with the long-anticipated problem of IPv4 address exhaustion.
- IPv6 allows to access 2^128 addresses. The IPv6 specification can be found on the Web at http1 2015.
- The IPv6 addressing architecture can be found on the Web at http2 2015. The document includes the IPv6 addressing model, text representations of IPv6 addresses, and definition of IPv6 unicast addresses, anycast addresses, multicast addresses, and IPv6 node's required addresses.

1.1 Cyber-Physical Systems (cont.)

Against this background cyber-physical systems go beyond the traditional systems employed in industry with regard to their complexity, requiring a close networking with the appropriate disciplines.

This makes three basic technologies essential for cyber-physical systems:

- **Embedded computing systems (ECSs)**
- **Networking, information, and communication technologies (NICT)**
- **Sensing and actuating technologies (SAT)**

Therefore, the decreasing cost of computation, networking, and sensing provides the basic economic motivation embedding networking, information, and communication technologies in every industry and application.

Moreover, the exponential growth in computing power has launched extremely sophisticated computers at consumer electronics prices into the market. The same trends have vastly improved sensing and actuation technologies.

1.1 Cyber-Physical Systems (cont.)

Thus, computers and communication have become the universal system integrator that keeps large systems together which enable the composition of the cyber-physical systems infrastructure.

Hence, cyber physical systems have an advanced and complex system architecture that connects computing, networking, and the physical and cyber or virtual environment within one paradigm.

It provides services such as:

- **Control**
- **Information feedback**
- **Real-time monitoring**

as most essential actions to merge the interaction of the physical and the cyber worlds by integration and collaboration of computation, communication, and control.

1.1 Cyber-Physical Systems (cont.)

Against the background of technological innovations, it can be stated that cyber physical systems and the Internet of Things become closer to each other with many similarities. Both are sensing, actuating, computing, transmitting information, and using interaction technologies to merge the cyber and the physical worlds.

But nowadays also some differences can be recognized.

The Internet of Things emphasizes the connection of things with networks, while cyber-physical systems emphasize the integration of computational and physical element information.

With regard to this remarks, ubiquitous computing is of crucial interest, because it is not only supporting global ubiquity to interlink systems to produce an omnipresent service architecture but rather to support context-based ubiquity, which can be understood as situated access versus mass access which may reduce human interaction in automation.

1.1 Cyber-Physical Systems (cont.)

- Thus, the term cyber physical system refers to the integration of computation with the physical and the cyber world's whereby things can be sensed through ubiquitous sensors and preprocessed by ubiquitous computing.

Therefore, the architecture of cyber physical systems should be ubiquitous and/or an integration of paradigms. such as:

- **Ambient intelligence:** referring to electronic environments sensitive and responsive to the presence of things/objects.

In an ambient intelligent world, devices work together supporting things and/or people doing their tasks, everyday life activities, etc., in an easy way using information and intelligence hidden in the network connecting these devices through the Internet of Things requesting for ubiquitous computing which allows massive networking of computers, sensors, actuators, and radio modules where things/objects communicate with each other.

1.1 Cyber-Physical Systems (cont.)

- **Disappearing computers**: referring to the miniaturization of devices and their integration into the environment. Thus, the devices disappear into our surroundings until only the user interface remains perceivable by users.
- **Pervasive computing**: often synonymously called ubiquitous computing, describes an emerging field of research that brings in revolutionary paradigms for computing models in the twenty-first century.
- **Post-PC era**: market trend involving a decline in sales of PCs in favor of post-PC devices, which include mobile devices such as smartphones and tablet computers. These devices emphasize portability and connectivity, including cloud-based services, more focused apps to perform tasks, and the ability to synchronize information between multiple devices seamlessly.
- **Ubiquitous computing**: concept in software and computer engineering where computing is made to appear everywhere and anywhere.

1.1 Cyber-Physical Systems (cont.)

- In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. Hence, cyber-physical systems are usually fused with other related concepts such as:

sensing through sensors and sensor networks, actuating through actuators and actuator networks, algorithms to adopt the behavior of networked systems, ontologies to interlink the cyber-physical systems applications, as well as interoperability standards and human-machine interfaces (HMIs) with situational adequacy and ergonomic issues.

1.1 Cyber-Physical Systems (cont.)

Comparing embedded computing systems with cyber-physical systems, it can be stated that cyber-physical systems are the integration of computing and communication with physical and virtual processes with the objective to convey how to interact with the physical world to monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa.

Thus, cyber-physical systems obtain many benefits:

They can make systems safer and more efficient; they can reduce the cost of building and operating these systems; and they can allow individual machines to work together to form complex systems that provide new capabilities.

1.1 Cyber-Physical Systems (cont.)

The design of such systems, therefore, requires understanding the dynamics of computers, software, networks, and physical and virtual or cyber processes allowing to create new machines with complex dynamics and high reliability.

Moreover, it will allow being able to apply the principles of cyber physical systems to new industries and applications in a reliable and economically efficient way.

Thus, the consolidating technological advances are that embedded computing systems created networked embedded computing systems which bear cyber physical systems which finally converge to Internet of Everywhere, Data, and Services, as shown in Fig. 1.1 based on the report of Geisberger and Broy (2012).

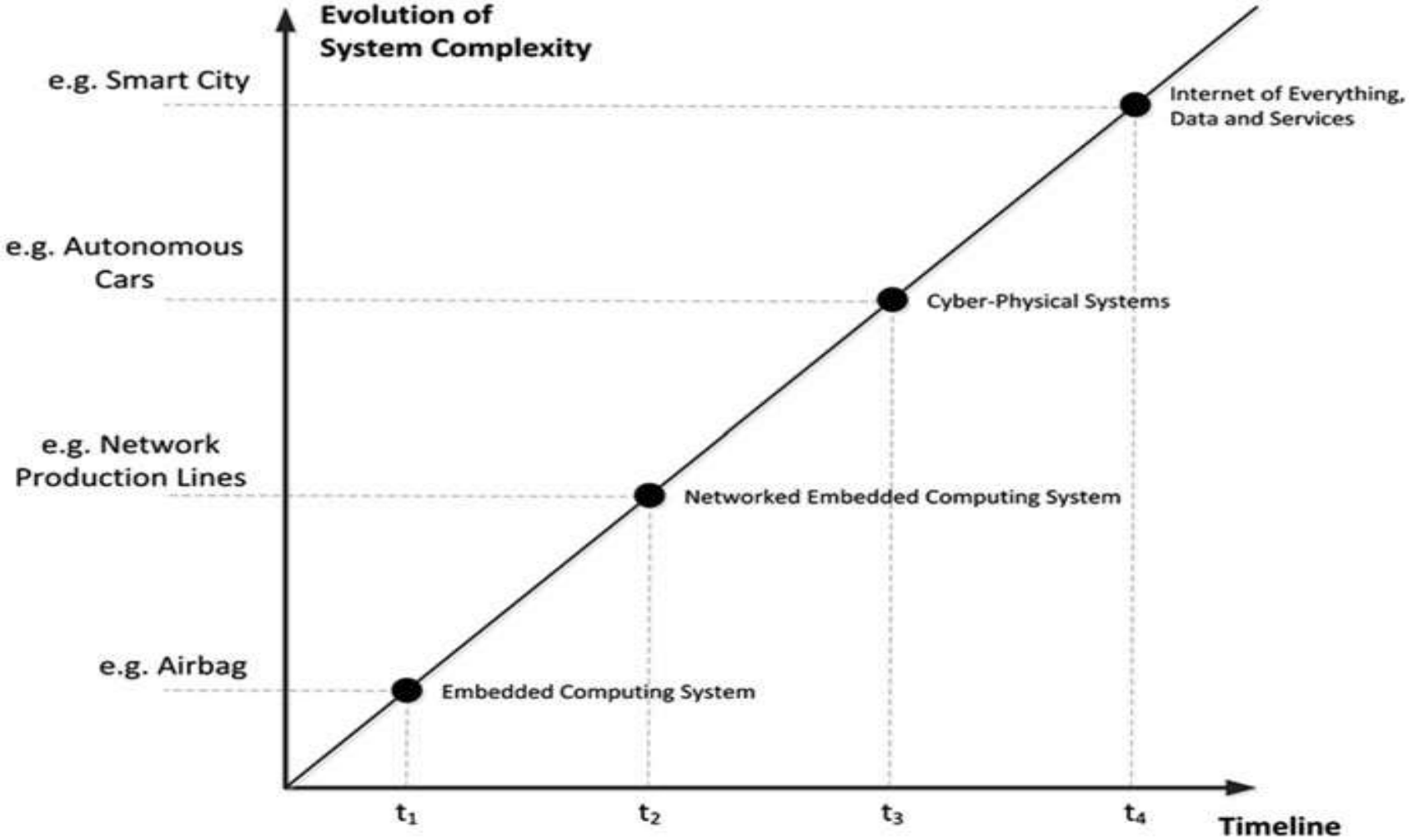

Fig.1.1 Evolution of Embedded Computing System (ECS) into the Internet of Things (IoT), Data, and Services

1.1 Cyber-Physical Systems (cont.)

The last two decades have launched a change in the direction of a digital revolution that has been transforming the industry.

This change is not a matter of choice; it is driven by fundamental, long-term technological and economic trends which will continue.

Thus, the challenges of cyber-physical systems as Fig. 1.1 Evolution of ECS into the Internet of Things (IoT), Data, and Services technological and economical driver result in different international activities to transform the industry like:

- Industrie 4.0: German initiative since April 2013 driven by the platform Industry 4.0.
- Advanced Manufacturing: US government initiative and funding program.
- Smart Manufacturing Leadership Coalition: nonprofit organization founded in 2012.
- Intelligent Manufacturing: national program driven by the Chinese Ministry of Science and Technology, released in March 2012.

1.1 Cyber-Physical Systems (cont.)

• Similar programs have been initiated by the European Union in their Horizon 2020 program in the Industrial Technologies Program which focuses on key enabling technologies such as advanced manufacturing and processing (production technologies) and the future of manufacturing by the British government and others.

Hence, cyber-physical systems acquire the designated role as backbone of advanced manufacturing (Industry 4.0.). Today's automation systems in industry will become intelligent, explorable, self-explanatory, self-aware, self diagnostic, and interacting assets in manufacturing systems which will be the basis for context-sensitive decision-making and automatic optimization of manufacturing systems and resources, usually making use of the ubiquitous plug and-produce paradigm.

1.1 Cyber-Physical Systems (cont.)

At the system level, cyber-physical systems map physical objects and corresponding virtual objects that communicate via ubiquitous information networks, whereby algorithms and services as well as dynamic integration of services and service providers and particularly information exchange will go across borders.

At the cyber level, which can be allocated in a cloud, embedding cloud computing within cyber-physical systems and Industry 4.0, data are collected in arbitrary and alterable information networks, 3D models and simulation models, documents, relations, and work conditions, and more will become available anywhere and anytime through ubiquitous or cloud computing.

1.1 Cyber-Physical Systems (cont.)

Ubiquitous computing is everywhere at the same time meaning omnipresent, making computing an embedded, invisible part of today's life. Tiny computing devices which vanish into the environment are required to introduce ubiquitous computing creating a completely new paradigm of a computing environment for heterogeneous sets of devices, including invisible computers embedded in everyday things/objects like automation devices, cans, clothes, cups, home devices, mobile devices, personal devices, security devices, vehicles, wall-size devices, wearable devices, and more, situated in the environments, inhabited buildings, secured areas, production facilities, and more.

Cloud computing is a metaphor on utility and consumption of computing resources. It involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources.

1.1 Cyber-Physical Systems (cont.)

The main consolidation of a typical cyber-physical system can be seen in integrating the dynamics of physical processes with those of the software and networking, providing abstractions and modeling, design, and analysis techniques for the integrated whole, which finally result in the so-called cyber-physical systems concept map, shown in Fig. 1.2.

From Fig.1.2 cyber-physical systems are primarily allocated as an engineering discipline, focused on technology, with strong foundation in mathematical abstractions.

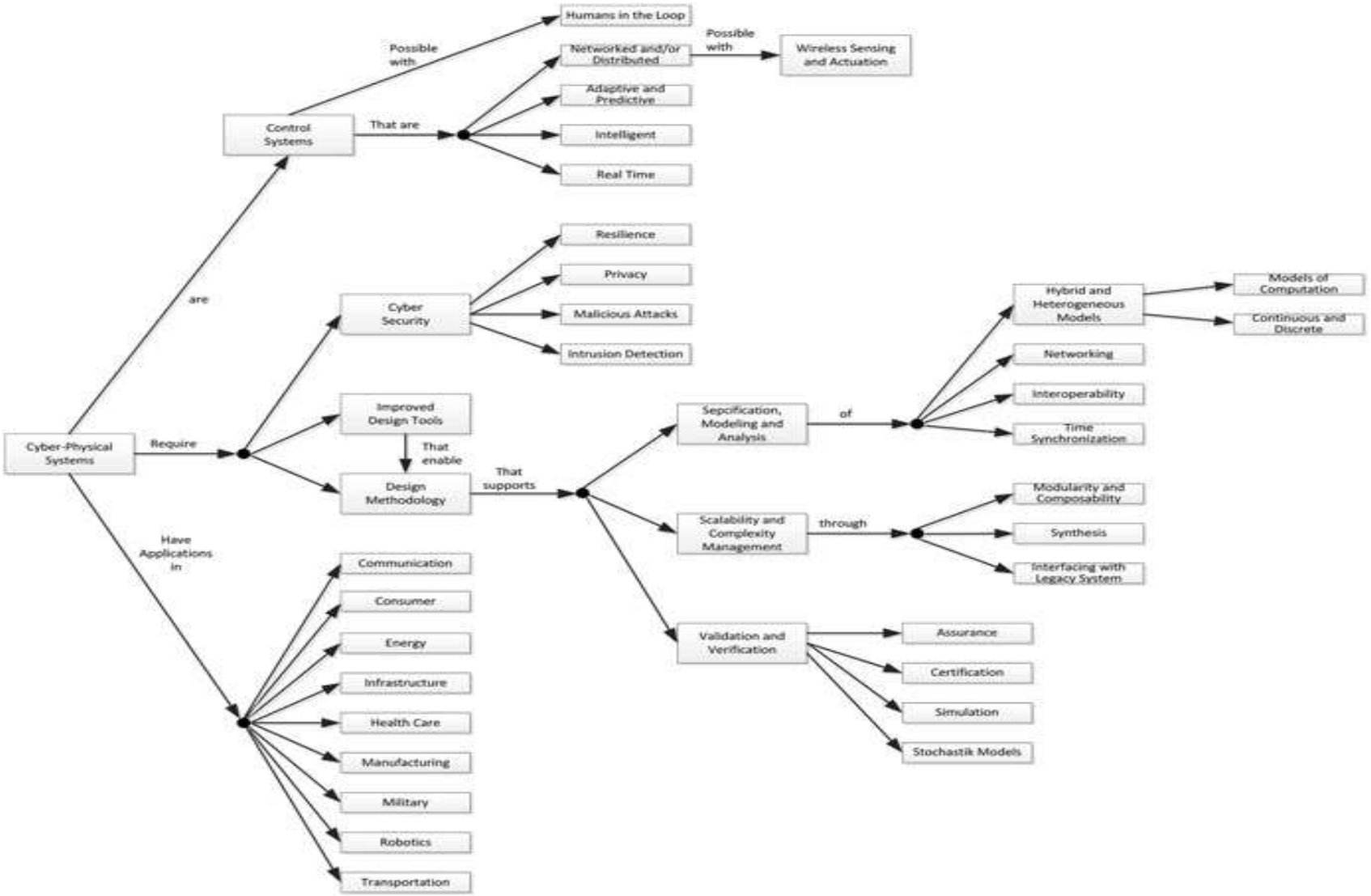

Fig. 1.2 Cyber-physical systems concept map

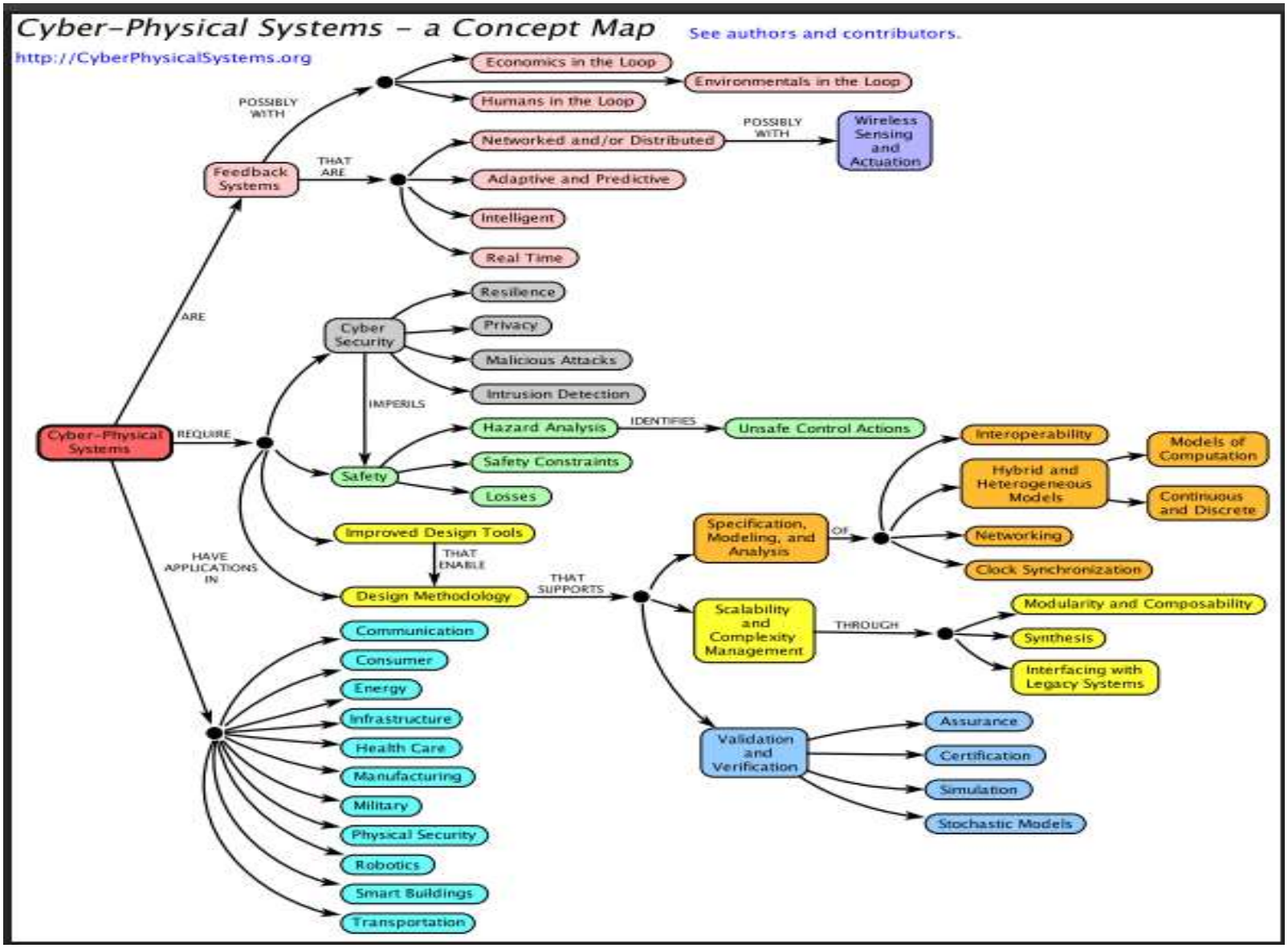

Fig. 1.2 Cyber-physical systems concept map

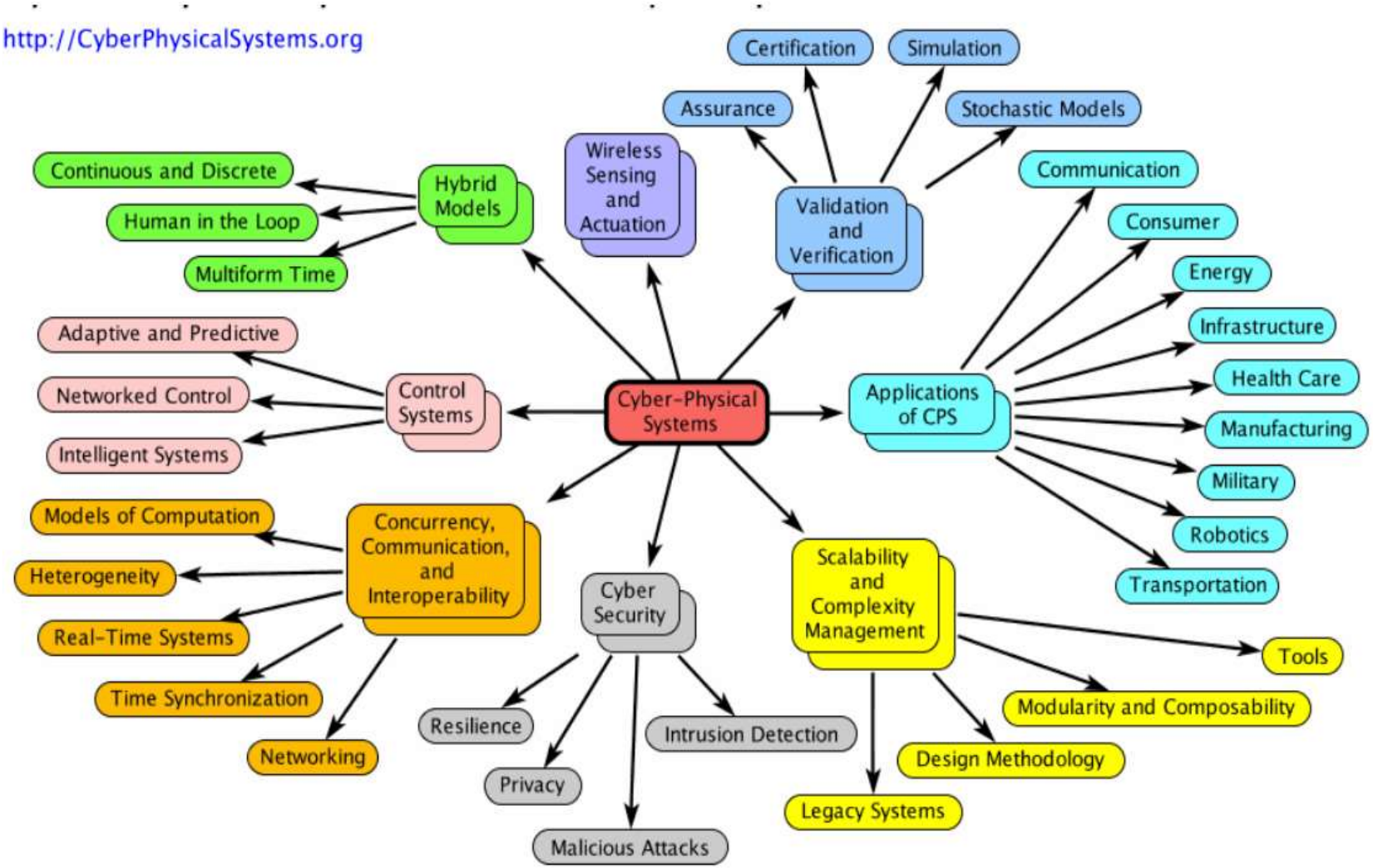

Fig. 1.2 Cyber-physical systems concept map

1.1 Cyber-Physical Systems (cont.)

Technical challenge is to conjoin abstractions that have evolved for modeling physical processes like differential equations, stochastic processes, and more with abstractions that have evolved in computer science with regard to algorithms and programs, which provide a procedural epistemology.

Former abstractions focus on the dynamic evolution of system state over time, whereas the latter focus on processes of transforming data. Computer science abstracts away core physical properties, particularly passage of times that are required to include the dynamics of the physical world in the domain of discourse.

Thus, cyber-physical systems have foundational characteristics like:

- Performance: with regard to control engineering
- Capacity: with regard to information theory
- Information processing: with regard to sensor networks
- Real-time communication: with regard to networking
- Formal methods: with regard to computer science
- Middleware: with regard to software engineering